RESPONSE

Claims Status

Claims 1 – 21 were originally filed in this application. A restriction requirement was issued on February 7, 2005, and in a response thereto, Applicant elected to pursue claims 1 – 18 in this application. An office action was issued on September 19, 2005, rejecting claims 1 – 18, and Applicant filed a response thereto on December 7, 2005, in which claims 1 – 4, 9 , 11, 16 and 18 were amended. A final office action was issued on January 27, 2006, maintaining the objections of the previous action, and Applicant filed a response thereto on March 21, 2006, in which claims 1 – 4, 11 and 18 were amended. The response was entered into the record on April 19, 2006, in conjunction with a Request for Continued Examination. An office action was issued on May 23, 2006, and included new grounds for rejections of claims 1 – 18. In response, Applicant filed an Amendment and Response on August 8, 2006, in which claims 1 – 4, 11, 15 and 18 were amended. A final office action was issued on October 23, 2006, citing a new reference and new grounds for rejection. Applicant hereby submits this Amendment and Response in which claims 1 – 4, 11 and 18 are amended. Support for the amendments can be found throughout the originally filed specification and claims, and, for example, at paragraphs [0050] – [0054] of the application as published. No new matter has been added.

Claim Rejections

In the current action, claims 1 – 18 were rejected under 35 U.S.C. § 103(a) as allegedly being unpatentably obvious in view of U.S. Patent Serial No. 6,233,577 to Ramasubramani et al. ("Ramasubramani") in view of U.S. Patent Serial No. 6,161,139 to Win et al. ("Win") and U.S. Patent Serial No. 6,577,733 to Charrin ("Charrin").

Applicant respectfully submits that the claims as amended are patentable over the cited references.

Ramasubramani

Ramasubramani is directed generally to a centralized certificate management proxy server useful for mobile devices. The proxy server facilitates "obtaining certificates asynchronously, apart from the tradition of obtaining certificates in local devices that normally have sufficient computing power." Col. 7, line 63 – 66. The Ramasubramani proxy server stores certificates in a table at the proxy server so that a mobile device can make use of the certificates via the proxy server even if it lacks sufficient processing power to do so.

Each Ramasubramani mobile device "has its own unique device ID that corresponds to a subscriber ID." Col. 7 lines 1-5. The user's account on the proxy server is "indexed by the device ID or the subscriber ID and identified by an address identifier such as a URL" and "compris[es] user info, a certificate list, and a private key list." Col. 7 lines 10-14.

A user can use a PC (not the mobile device) to access the user's account on the proxy server: "the user may use the PC which has preferably a sufficient computing power and equipped with a more familiar HTML browser to establish a communication session using HTTP and the URL to the account." Col. 8 lines 54-57. When accessing his account from a PC, the user employs a username and password: "If the entered username and password are matched, the authorization is granted so that the user or (sic) the PC is permitted to access the account. Col. 8 lines 63-65.

Win

Win is directed generally to role-based authentication services for administrative functions within web-based applications. To perform a given function, a user logs into a registry server using a user ID and a password, and the registry server authenticates the user. Col. 9 lines 25-35. An authentication service then retrieves user profile information based on the roles attributed to the user and application privileges associated with the roles. Col. 10 lines 29-33. The authentication service "creates a 'user cookie' and a 'roles cookie' which are used to convey profile information to [a] browser. Col. 10 lines 36-38.

Charin

Charin generally describes an affinity card for cashless gambling. According to Charin, a secure cashless gaming system includes gaming devices "which may or may not be connected to a central host network" and that "includes an intelligent data device reader which is uniquely associated with a security module interposed between the intelligent data device reader and the gaming device processor." Col. 3 lines 15-21. Users are issued "a portable data device (such as a smart card) bearing credits" that permit players to play the devices. Col. 3 lines 21-23. The portable data devices are "authenticated" before a gaming session is allowed to begin. Col. 3 lines 23-25. The data device reader at each of the gaming devices "monitors gaming transactions and preferably stores the results" "in a secure format by a portable data extraction unit, or else for transfer to a central host network." Col. 3 lines 25-29.

Claims 1 – 18

As amended, independent claims 1, 2 and 3 each recite in part, locating "session context information based on [a] device identifier" that was "associated with the device identifier during a previous wireless session," locating "access privileges" and "using the located access privileges and data contained in the session context information to authorize a current session between the device and the resource." As amended, independent claims 4 and 11 each recite, in part, "locating session context information associated with [a] device identifier, the session context information associated with a previous wireless session between the device and the resource and including access privileges associated with a cluster of users" and "providing the session context information for use in a current session between the device and the resource." As amended, independent claim 18 recites in part, "computer program instructions" that "cause a digital processor to" "locate . . . session context information associated with [a] device identifier, the session context information associated with a previous wireless session between the device and the resource" and "providing the session context information for use in a current session between the device and the resource."

The Office Action notes that Ramasubramani does not teach the use of session context information associated with a device identifier during previous wireless sessions. Office Action, page 4. To provide this claim element, the Office Action relies on Charrin, which, as noted above, describes an affinity card system for gaming devices that records details of historical gaming sessions. However, neither Ramasubramani nor Charrin describe using data contained in the session information to authorize a subsequent session between a wireless device and a resource. In contrast, Applicants claim "session context information" that is "associated with" or "assigned to" a "device during a previous wireless session" and is used to authorize "a current session between the device and the resource." By maintaining session context information for individual connections (such as storing an IP address attributed to a particular device ID at a gateway server, for example) and making that context information available to devices in subsequent sessions, a user can move a mobile device among numerous access points without requiring re-registration to the network. As described above, Ramasubramani maintains user and site-specific digital certificates, not session context information. While Charrin stores "session information" on a portable device, the Charrin session information is only used to track the gaming and spending habits of frequent gamblers, not for authenticating the devices themselves. In fact, Charrin explicitly states that "each time an attempt is made to initiate a gaming session . . . an authentication process is performed to ensure that the correct intelligent data device reader and correct security module are present." Col. 3 lines 39-44. Particularly, Fig. 16 and the corresponding text describe how, for each of the three types of cards, and for each operation, "the card is cross-authenticated with the intelligent data device reader and, more specifically, with the security and authentication module." Col. 11 lines 50-52. Thus, even in combination with Charrin, Ramasubramani could not use stored session information for authentication because Charrin teaches that a new authentication process is performed for each session. A Ramasubramani-Charrin combination would not alleviate the need for re-authentication and the provisioning of new network context information when users roam among wireless access points, because this is a result not contemplated by either reference.

The erroneous application of Charrin to Ramasubramani is also evident, for example, with respect to claim 8, which recites, in part, "the session context information includes an internet protocol address assigned to the device in the previous wireless session." As mentioned, the Office Action states that Ramasubramani does not have session context information. The Office Action later suggests, however that claim 8 is obvious because Ramasubramani, as modified by Charrin, has an "internet protocol address assigned to the device in the previous secure session." Office Action, page 8. The elements of claim 8 identified in the Office Action as "internet protocol addresses" from Ramasubramani, however, are uniform resource locators associated with different destinations, not a specific device, and the "session information" from Charrin describes gaming activities. Neither teaches or suggests an internet protocol address for a device assigned in a previous session. The proposed combination of Ramasubramani and Charrin therefore would not have all of the limitations of claim 8 because neither

Ramasubramani nor Charrin stores session context information from a previous session, let alone an internet protocol address.

Applicant respectfully submits that it is improper for the Office Action to pick and choose unrelated elements from the different references regardless of their applicability to each other absent any suggestion in the references to motivate one skilled in the art to do so. For example, combining Ramasubramani with Charrin might result in a personal data assistant for storing gambling results that also happens to include a web-enabled cellular telephone, even though one reference has virtually nothing to do with the other, and data from one feature has no applicability to the other. The mere conjecture that a proxy server for wireless devices could potentially be combined with a gambling affinity card system does not suggest which features that might be useful to take from each, whether these features would even be able to operate together, or how the claimed invention might possibly result.

Win does not cure the deficiencies of Ramasubramani or Charrin. Win provides role-based application privileges to browser users via cookie files. Win makes no mention of re-using session-based context information, let alone providing authentication to users of wireless networks.

As such, Applicant respectfully submits that independent claims 1-4, 11 and 18, as well as those claims that depend therefrom, are patentable over the cited references.

CONCLUSION

Applicant respectfully requests that the Examiner reconsider the application and claims in light of this Response, and respectfully submits that the claims are in condition for allowance. If the Examiner believes, in his review of this Response or after further examination, a telephonic interview would expedite the favorable prosecution of the present application, the Applicant's attorney would welcome the opportunity to discuss any outstanding issues, and to work with the Examiner toward placing the application in condition for allowance.

Respectfully submitted,

Date: December 22, 2006
Reg. No. 56,401

Joel E. Lehrer
Attorney for Applicant
Goodwin Procter LLP
Exchange Place
Boston, Massachusetts 02109
Customer No. 051414

Tel. No.: (617) 570-1057
Fax No.: (617) 523-1231